

Secure Mobility – SandBlast Mobile from O₂

O₂ business

A product sheet from O₂

Protect your mobile workforce against known and unknown threats

What protection do you have in place to ensure your mobile devices – and the business critical information they contain – are protected against unwanted visitors?

Employees demand ever-greater remote access to corporate data. But this can easily open up security gaps in your infrastructure. Cyber criminals target mobile devices because they offer so much access to potentially sensitive information. This could be via a device's on-board microphone and camera, or by viewing the user's text history, call history, app data, documents and more. Traditional safeguards like PINs, passwords, static policies and containers provide little protection against today's sophisticated cyber threats. And these measures are unable to tell you if an attack is underway.

Secure Mobility – SandBlast Mobile from O₂, powered by Check Point, enables organisations to maintain continuous security across their entire mobile environment. SandBlast Mobile detects cyber threats targeting mobile Operating Systems (OS), applications and networks. Through a combination of cloud-based and device-based services, SandBlast Mobile provides always-on, always up-to-date protection for mobile device users – by blocking malicious activity, and stopping bot attacks before they cause any damage.

SandBlast Mobile's intelligent threat detection technology monitors multiple attack vectors. It looks at a device and its environment in context – an essential requirement of a successful mobile device protection strategy.

Mobile threats: the reality

According to the latest insights, mobile device usage continues to grow¹:



The threats are growing too²:



¹ Mobile in the enterprise – why traditional security tactics such as firewalls, IPS and anti-malwares are no longer enough, September 2017

² The growing threat of mobile device security breaches, a global survey of security professionals, April 2017

Why choose Secure Mobility?



Compatible with existing Mobile Device Management (MDM) solutions

MDM solutions can help you manage, configure and monitor mobile devices. SandBlast Mobile helps you actively protect your mobile devices, because it adds the capabilities you need to ensure malware protection, as well as offering extra safeguards against malicious data going into and out of any device.



Real-time protection

SandBlast Mobile, a mobile threat defence solution to protect employees' devices from; malware attacks via infected apps, man-in-the-middle attacks through comprised Wi-Fi networks, vulnerabilities and malicious links sent via SMS messages.



Maintain full visibility with a single, integrated platform

SandBlast Mobile threat analysis provides real-time intelligence about the security status of your mobile devices. Information can be fed into existing enterprise Security Information and Event Management (SIEM) platform. While the online SandBlast Mobile portal can provide device-level threat information to quickly control and eliminate risks.



Deploy advance mobile protection with ease

Whether you support 30 or 300,000 devices, integrating SandBlast Mobile with your MDM solution is fast and straightforward. It is also designed to be non-intrusive. It's easy for users to keep work data secure, while maintaining their personal privacy and without compromising device performance.

What you get with Secure Mobility

- **Mobile App:** provides a link to the cloud-based Behavioural Risk Engine (BRE).
- **BRE:** Utilises multiple data sources, including threat emulation, advanced static code analysis, app reputation and machine learning to identify threats.
- **Integration:** SandBlast Mobile links directly with an MDM or SIEM platform for enterprise wide integration.
- **Easy control:** Online admin portal for easy application of business wide policies and real-time reporting on your entire real-estate.

Features at-a-glance

- On-device protection against Malware and Cyber-threats.
- Detection and blocking of SMS phishing attacks.
- App analysis to detect known and unknown threats.
- Network monitoring against malicious behaviours.
- Supported on smart phones and tablets running Android and iOS.
- Clear end-user alerts with remediation recommendations.
- Seamless deployment and adoption of policies.
- Cloud-based admin portal providing detailed reporting.

Why O₂?

With a rich heritage in the arena and diverse portfolio of mobility experience, our mobile-first strategy makes us an ideal partner for the growing mobile workforce, who demand the agility of flexible working, while you demand information integrity and security, which historically have not been compatible.

O2 currently manage more than 100,000 iOS, Android, Windows and BlackBerry devices for Enterprise customers in the UK. Our expert teams are led by PRINCE2 and ITIL3 accredited project managers that can handle any mobility challenge.

We are the only UK mobile provider to achieve CAS(T) security certification on our mobile and WAN networks making us the safe choice in every way.

We'll support you all the way

To learn more about safeguarding your mobile devices with SandBlast Mobile and O2, chat with your O2 Account Manager. Alternatively, call us on **01235 433507** or visit **o2.co.uk/enterprise**.

